

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-258059

(43)Date of publication of application : 21.09.2001

(51)Int.Cl.

H04Q 7/22

H04Q 7/28

H04L 12/28

(21)Application number : 2001-029555

(71)Applicant : LUCENT TECHNOL INC

(22)Date of filing : 06.02.2001

(72)Inventor : DAVIES STEPHEN WILLIAM
VANDERVEEN MICHAELA C

(30)Priority

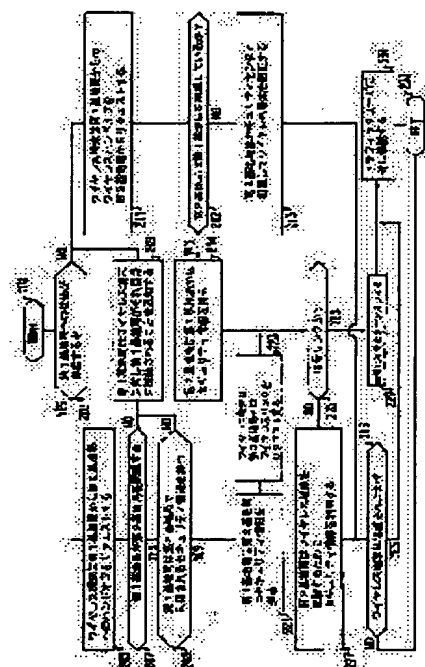
Priority number : 2000 501168 Priority date : 09.02.2000 Priority country : US

(54) EXECUTION METHOD FOR HANDS-OFF PROCEDURE IN NETWORK

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for reducing the installation cost of a network by simplifying the architecture of the network.

SOLUTION: The method where hands-off procedure in a network having 1st and 2nd base stations and a wireless mobile terminal is executed, is characterized in that the method includes a step (A), where a request of hand-off from the 1st base station to the 2nd base station is received from the mobile terminal and a step (B), where the 1st base station transmits security information to the 2nd base station.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

BEST AVAILABLE COPY

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2001-258059
(P2001-258059A)

(43)公開日 平成13年9月21日(2001.9.21)

(51)Int.Cl. ⁷	識別記号	F I	デマコト* (参考)
H 0 4 Q 7/22		H 0 4 L 12/28	3 0 0 Z
7/28			3 1 0
H 0 4 L 12/28	3 0 0	H 0 4 Q 7/04	K
	3 1 0	H 0 4 B 7/26	1 0 7

審査請求 未請求 請求項の数22 OL (全 9 頁)

(21)出願番号 特願2001-29555(P2001-29555)

(22)出願日 平成13年2月6日(2001.2.6)

(31)優先権主張番号 09/501168

(32)優先日 平成12年2月9日(2000.2.9)

(33)優先権主張国 米国(US)

(71)出願人 596077259
ルーセント テクノロジーズ インコーポ
レイテッド
Lucent Technologies
Inc.
アメリカ合衆国 07974 ニュージャージ
ー、マレーヒル、マウンテン アベニュー
600-700

(74)代理人 100081053
弁理士 三俣 弘文

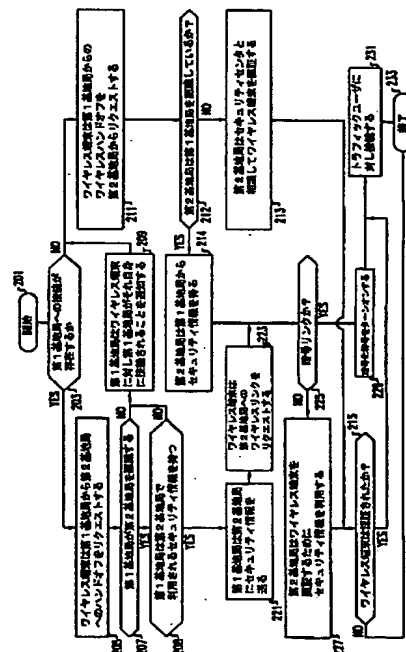
最終頁に続く

(54)【発明の名称】 ネットワーク内のハンドオフの実行方法

(57) 【要約】

【課題】効率的なネットワーク内のハンドオフの実行方法を提供する。

【解決手段】 本発明によれば、第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、（Ａ）第１基地局から第２基地局へのハンドオフのリクエストを移動端末から受信するステップと、（Ｂ）前記リクエストの応答して、第１基地局から第２基地局にセキュリティ情報を転送するステップと、を有することを特徴とする。



【特許請求の範囲】

【請求項1】 第1と第2の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

(A) 第1基地局から第2基地局へのハンドオフのリクエストを移動端末から受信するステップと、

(B) 前記リクエストの応答して、第1基地局から第2基地局にセキュリティ情報を転送するステップと、を有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項2】 前記セキュリティ情報は、少なくともランダム数と、第1基地局、第2基地局ではなく移動端末から得られた認証情報とキーとをからなる組を含むことを特徴とする請求項1記載の方法。

【請求項3】 前記セキュリティ情報の少なくとも一部を用いて、前記第2基地局への移動端末を有効にすることを特徴とする請求項1記載の方法。

【請求項4】 前記セキュリティ情報は、前記第1基地局が受信したセキュリティ情報のすべてではなく、前記リクエストにตอบสนองして、前記第1基地局から第2基地局に転送されることを特徴とする請求項1記載の方法。

【請求項5】 前記第1基地局が受信したセキュリティ情報の全ては、ワイヤレス移動端末の認証システムから受領することを特徴とする請求項4記載の方法。

【請求項6】 前記第1基地局が受領したセキュリティ情報の全ては、第3基地局から受領することを特徴とする請求項4記載の方法。

【請求項7】 前記(B)のステップは、(B)ステップを実行する前に第1基地局が第2基地局を認識しているときのみ行われることを特徴とする請求項1記載の方法。

【請求項8】 (C)前記第1基地局とワイヤレス端末が暗号化リンクを用いて通信しているときに、第2基地局とワイヤレス端末との間に暗号化リンクを初期化するステップを有し、

前記第2基地局は、第2基地局とワイヤレス端末との間の暗号化リンクを初期化する際に、前記第1基地局から第2基地局へ転送されたセキュリティ情報を用いることを特徴とする請求項1記載の方法。

【請求項9】 第1と第2の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

(A) 第1基地局から第2基地局へのハンドオフのリクエストを、ワイヤレス端末から送信するステップと、

(B) 前記第2基地局が第1基地局とのハンドオフに関連する旨のリクエストを受領する前に、第2基地局が第1基地局を認識しているときに、前記ワイヤレス端末で応答を受領するステップと、

(C) ユーザトラフィック用のワイヤレス端末を第2基地局に接続するステップとを有することを特徴とするネ

ットワーク内のハンドオフの実行方法。

【請求項10】 前記実行されたハンドオフは、前記第1基地局から第2基地局へ転送されたワイヤレス端末に関する情報を用いることを特徴とする請求項9記載の方法。

【請求項11】 前記情報はセキュリティ情報であることを特徴とする請求項10記載の方法。

【請求項12】 前記情報はセキュリティセンタから受領したセキュリティ情報であることを特徴とする請求項10記載の方法。

【請求項13】 前記情報は、前記第1基地局と第2基地局以外の第3基地局から受領したセキュリティ情報であることを特徴とする請求項10記載の方法。

【請求項14】 前記情報はセキュリティ情報であり、(i)パスワードと、(ii)チャレンジ-応答対と、(iii)チャレンジ-応答暗号化キー-tuple からなる組からの少なくとも1つを含むことを特徴とする請求項10記載の方法。

【請求項15】 前記情報は基地局間の通信用のネットワークを介して受領したセキュリティ情報であることを特徴とする請求項10記載の方法。

【請求項16】 前記(C)ステップは、前記第1基地局とワイヤレス端末が、ハンドオフリクエストの前に暗号化リンクを用いて通信しているときに、前記第2基地局とワイヤレス端末との間の暗号化リンクを初期化するステップを有し、前記第2基地局は、前記第2基地局とワイヤレス端末との間の暗号化リンクを初期化する際に、前記レスポンスの一部として第1基地局から第2基地局へ転送されたセキュリティ情報を用いることを特徴とする請求項10記載の方法。

【請求項17】 第1と第2の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

(A) 第1基地局から第2基地局へのハンドオフのリクエストを、ワイヤレス端末から送信するステップと、

(B) 前記リクエストを受領する前に、第2基地局が第1基地局を認識していなかった場合には、第1基地局から与えられる情報を利用することなく、ワイヤレス端末が第2基地局に接続されなければならないという指示をワイヤレス端末で受領するステップを有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項18】 前記情報はセキュリティ情報であることを特徴とする請求項17記載の方法。

【請求項19】 前記情報はセキュリティセンタから受領したセキュリティ情報であることを特徴とする請求項17記載の方法。

【請求項20】 前記情報は、前記第1基地局と第2基地局以外の第3基地局から受領したセキュリティ情報であることを特徴とする請求項17記載の方法。

【請求項21】 第1と第2の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

(A) 第1基地局と第2基地局との間のハンドオフのリクエストをワイヤレスから第2基地局が受領するステップと、

(B) 前記リクエストを受領する前に、第2基地局が第1基地局を認識しているときには、容易なハンドオフを実行するステップと、

(C) 前記リクエストを受領する前に、第2基地局が第1基地局を認識していなかった場合には、容易でないハンドオフを実行するステップと、を有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項22】 前記(B)のステップは、前記第1基地局から第2基地局へセキュリティ情報を転送するステップを含むことを特徴とする請求項21記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はワイヤレス通信に関し、特に、ワイヤレス通信サービスを提供するネットワークの認定されたユーザのみがネットワークへのアクセスを許されるようなシステムに関する。

【0002】

【従来の技術】 従来のワイヤレスシステムは、認定されたワイヤレス端末のみがワイヤレスネットワークにアクセスすることができる。ワイヤレス端末がネットワークへアクセスできるようにするために、ワイヤレス端末は認定(認証)されなければならない。ここで本明細書において用語「認定(認証)」は、権限があると主張するエンティティを証明(認証)するプロセスである。電話の呼が持続する間、例えば呼が開始され、その後ワイヤレス端末がネットワーク内の規定された境界で移り変わると、複数回認証が必要とされる。

【0003】 認証は、ワイヤレス内に登録された秘密情報から抽出された情報と、ネットワーク内のそれ以外の場所にある情報から抽出された情報とを比較することにより行われる。通常、比較する位置に最も近い場所にある抽出された情報の記憶場所からの一度の呼の間に、特定のワイヤレス端末に対して新たな認証が必要とされることに、この抽出された情報は送信される。

【0004】 ワイヤレスは基地局とエアリンクを介して通信される。基地局が比較場所がない場合には、基地局はワイヤレス端末から情報を比較場所に送らなければならない。抽出された情報が登録されているネットワーク内の場所は、いわゆるビジターロケーションレジスタ(visitor location register: VLR)である。この抽出された情報は、いわゆるホームロケーションレジスタ(home location register: HLR)、あるいは別の認証センタ(特定のネットワークのデザインによっては)で生成される。ワイヤレス端末が第1のVLRによ

りサービスされる領域を、第2のVLRによりサービスされる領域と区別するようなネットワーク境界に近づくにつれて、第1VLRは、抽出された情報を第2VLRに送信する。別の構成として第2VLRは、HLRからそれ自身で抽出した情報を得る。HLRは、HLRにより直接サービスされる領域でワイヤレス端末が最初に電源が入れられたときには、VLRとして機能する。

【0005】 好ましくないことに、様々な特殊なエンティティが存在し、複雑な制御手順が必要とされるために、従来のネットワークのコストは高かった。

【0006】

【発明が解決しようとする課題】 本発明の目的は、ネットワークのアーキテクチャーを単純化し、ネットワークの接地コストを低減する方法を提供する。

【0007】

【課題を解決するための手段】 前記課題を解決するために本発明は、ネットワーク内の規定された境界を基地局レベルまで押し下げることにより達成できる。しかしそうした結果は、ワイヤレス端末がある基地局から別の基地局へ通信を切り替えることに認証が必要とされることになる。言い換えると、規定された境界を基地局レベルまで押し下げた後、ある基地局から別の基地局へワイヤレス端末のハンドオフが存在することに、ネットワーク境界をまたぎ、認証が必要とされる。このような認証を効率的の個々なために、本発明によれば、セキュリティ情報すなわち抽出された情報は、ある基地局から直接別の基地局の転送される。ここで「直接」とは、情報が他の基地局の相互接続バスを構成するネットワークの他の干渉ノードを介して転送される場合でも、抽出された情報の他のソースにアクセスしないことを意味する。好ましいことに単純化されたネットワーク、すなわち制御の観点から回送を低減させたネットワーク、例えばHLRと相互接続を有する基地局ネットワークのみを必要とするネットワークは、性能の劣化を最小に押さえながら、例えばハンドオフプロセスの間、遅延の増加を最小に押さえながら採用される。

【0008】 更に具体的に説明すると、本発明の一実施例においては、ワイヤレス端末からサービスリクエストを最初に受領した第1基地局は、中央セキュリティノード、例えばHLRから認証情報を要求し、それに応答して少なくとも1つ、通常複数のセキュリティ情報を受領する。セキュリティ情報の組は、パスワード、チャレンジ-応答対、チャレンジ-応答cipher key tuple等である。第1基地局から第2基地局へのハンドオフの時には、第1基地局は第2基地局に中央セキュリティノードから受領したセキュリティ情報の組の少なくとも1つを送る。その後この第2基地局は、第1基地局から受領したこの情報を用いて、ワイヤレス端末を認証するおよび/または暗号化通信に関わる。

【0009】

【発明の実施の形態】図1は本発明によるネットワーク構成を表す。同図には、(a)ワイヤレス端末101と、(b)基地局103-1から103-Nを含むN個の基地局103と、ここでNは、2以上の整数である、(c)アンテナ105-1から105-Nを含むの個のアンテナ105と、(d)構造物107-1から107-Nを含むN個の構造物107と、(e)セル109-1から109-Nを含むN個のセル109と、(f)ネットワーク111と、(g)基地局認証ユニット113と、(h)通信リンク115-1から115-Nを含むN個の通信リンク115と、(i)通信リンク117、通信リンク121と、(j)セキュリティセンタ119とが示されている。

【0010】ワイヤレス端末101は、複数の基地局と通信でき、この基地局は検出可能な十分な信号強度でもって信号を送信し、ワイヤレス端末101の現在の位置で通信できる。十分な強度の信号が特定の基地局に対し検出されると、ワイヤレス端末101はその基地局と通信を行う。ワイヤレス端末101により採用されたワイヤレス（無線）リンクとプロトコル、すなわちエアインタフェースの種類は、本発明にとって本質的要素をなすものではないが、ワイヤレス端末101により採用されるワイヤレスリンクとプロトコルは、基地局103に採用されるのと同じのものでなければならないが、当業者の必要により、いかなる種類のものでも良い。

【0011】ワイヤレス端末101は複数の基地局と通信を行うことができる。例えばワイヤレス端末101は、単一の受信器であり、ワイヤレス端末101が信号を受信すると、それに現在サービスしている基地局との情報交換で占有されていない場合には、ワイヤレス端末101に到達するのに十分な強度の信号を有する他の基地局から信号を受信することができる。別の構成例として、ワイヤレス端末101は、複数の基地局から同時に、例えばワイヤレス端末101内の複数の並列受信器を採用することにより信号を受信することができる。さらにまた別の構成例として、ワイヤレス端末101は、複数の受信器であるが、受信器の数はワイヤレス端末101が、その現在いる場所で十分な強度の信号を受信できる基地局の数以下であり、その結果ワイヤレス端末101は、ある基地局からの信号を得るために、その受信器の少なくとも1つに対し走査を実行する必要がある。

【0012】基地局103は、以下の説明を除いて従来の基地局である。まず第1に基地局103は、基地局間通信に対し専用ネットワークに接続される必要はない。その代わりに基地局103は、共有公衆ネットワーク、例えばインターネットのようなIPベースのネットワークを採用することができる。第2に、各基地局103は、「地図」情報を含む必要がない。その代わりに各基地局103は、「地図」情報の必要な部分のみを発見することができるればよい。好ましくは、基地局103は小

さなスペースに容易に組み込むことのできる小さな基地局である。例えば、専用の構造およびサイトを準備するのではなく、すでに利用可能なスペースに組み込まれた基地局である。好ましいことにこのような小型化は、

「地図」情報の必要な部分を見いだす機能と共に、新たなワイヤレス通信ネットワークの早急な構築が可能となる。さらにまたこのようなワイヤレス通信ネットワークは、そのアーキテクチャーがフレキシブルである、すなわち基地局は容易に追加、あるいは取り外すことができ、そしてさらにはまたそれを維持することも容易である。

【0013】各アンテナ105は、基地局103のそれぞれに接続されている。アンテナ105は、それぞれの基地局103により生成された信号を放射する。基地局103の1つとアンテナ105とそれに対応する1つの各組合せが、セル109の1つを生成する。図1のセル109の形状は、実際のセルの形状を示してはならず、単にセルに対する従来の概念を示したに過ぎない。実際の様々なセル109の形状は全て異なる。

【0014】各構造物107は、1つあるいは複数の基地局103を配置するための設備を有する。さらにまた構造物107は、アンテナ105を搭載する場所を提供する。例えばある構造物107は、1つの基地局103が未使用の場所に配置され、1つのアンテナ105が外部から取り付けられる既存の家である。

【0015】通信リンク117は、互いに通信する、および基地局認証ユニット113、セキュリティセンタ119と通信するための通信路を、基地局103に対し提供する。ネットワーク111は、様々なサブネットワークから構成される。さらにまた様々なサブネットワークは、異なる種類および異なるプロトコルを採用することも可能である。本発明の一実施例においては、ネットワーク111はパケットベースのネットワーク、例えばATMネットワーク、あるいはIPネットワークである。

【0016】各基地局103は、ネットワーク111にそれぞれ通信リンク115の1つを介して接続される。この通信リンク115はネットワーク111の一部とみなすことができる。例えば、ネットワーク111あるいは少なくともそのサブネットワークはIPネットワークであり、1つの基地局103は家である構造物107内に配置される。通信リンク115はインターネット接続であり、例えばケーブルテレビのライン、あるいは家から屋外への接続を介して行われるもので、これは他の基地局との通信を行う基地局により、あるいはインターネットのブラウジングを行うための家の所有者により共有される。

【0017】基地局認証ユニット113は、全て有効な基地局103のリストとそれに関連する情報、例えば基地局のセキュリティキーと別の識別子とあるいはアドレスを含む。基地局認証ユニット113にあげられた基地

局は、どの地点のものでも良い。しかし基地局は基地局認証ユニット113内のリストにあげられた場合のみ有効となる。同図には1つの装置としてしか示していないが、実際には基地局認証ユニット113はいくつかのパーツから構成され、これらは必ずしも地理的に同じ場所にある必要はない。さらにまた信頼性および性能を改善するために、基地局認証ユニット113の様々なパーツ、あるいは機能の一部あるいはすべてを複製することもできる。

【0018】基地局認証ユニット113はネットワーク111に通信リンク117を介して接続される。基地局認証ユニット113が複数のパーツから構築されている場合、あるいは複製されている場合には、通信リンク117は、ネットワーク111と様々なパーツとの間の必要な通信パスをカバーするものとして解釈できる。

【0019】セキュリティセンタ119は、サービスされている全ての有効ワイヤレス端末のリストを含む。さらにまた、セキュリティセンタ119はセキュリティ情報、例えば認証、チャレンジ応答対および/または各ワイヤレス端末に関連する暗号化キーを含む。セキュリティ情報は、必要によってはセキュリティセンタ119により基地局103に分配される。ワイヤレス端末はどの場所でも110内にリストアップすることができる。しかしワイヤレス端末は、セキュリティセンタ119内のリストに載ったとき初めて有効となる。図では1つの装置として示されているが、実際にはセキュリティセンタ119は数個のパーツから組み合わせられ、これらのパーツは必ずしも地理的に同一場所にある必要はない。さらにまた信頼性と性能を改善するために、セキュリティセンタ119の様々なパーツ、あるいは機能の一部、あるいはすべては複製することができる。

【0020】セキュリティセンタ119はネットワーク111に通信リンク121を介して接続される。セキュリティセンタ119が複数のパーツから構築されている場合、あるいは複製されている場合には、通信リンク121は、ネットワーク111と様々なパーツとの間の必要な通信パスをカバーするものとして解釈できる。

【0021】図2は、本発明により図1の基地局間のハンドオフを実行するフローチャートを示す。具体的に説明すると、ハンドオフのプロセスの一部として基地局は、基地局の「地図」の少なくとも一部、すなわち近隣の基地局のパターンとそれの関連情報を見だし更新する。特定の基地局により見いだされた地図の一部は、それがサービスしている呼がハンドオフされる近隣のものである。ローカル地図全体を見いだすために特定の基地局に対する近隣の基地局でもって、少なくとも1回のハンドオフが行われる。

【0022】本発明のプロセスは、ステップ201で開始され、ワイヤレス端末、例えばワイヤレス端末101(図1)が、ワイヤレス端末が通信している基地局、例

えば基地局103-1の無線リンクの信号が、別の基地局、例えば基地局103-2のそれよりも弱くなり、この別の基地局がより良好な無線リンクを提供するようになったために、ワイヤレス端末、例えばワイヤレス端末101はハンドオフをリクエストする。次に条件ブランチポイント203では、第1基地局、例えば基地局103-1への接続が存在するか否かを決定する。この理由は、第1基地局から受信した信号がワイヤレス端末で弱くなるか、あるいは第1基地局で受信したワイヤレス端末からの信号が弱くなり、その結果第1基地局とワイヤレス端末との間の接続がハンドオフが行われる前に難しくなるからである。ステップ203のテスト結果がYESの場合は、第1基地局とワイヤレス端末との間の接続が依然と存在していることを示し、制御はステップ205に移り、そこでワイヤレス端末は第1基地局から第2基地局、例えば基地局103-2へのハンドオフを要求する。別法としてワイヤレス端末は、第1基地局と第2基地局に対するワイヤレス端末で受信した信号強度の様々な測定値を、第1基地局に送り、この第1基地局はハンドオフに適した時間を決定する。そのため第1基地局は、ワイヤレス端末に対し第2基地局に接続するよう指示する。

【0023】次に条件ブランチポイント207は、第1基地局が第2基地局を認識しているか否かを決定する。すなわち第1基地局はその地図情報内にリストアップされている第2基地局を有しているか否かを決定する。このリスティングは、第1基地局と第2基地局の間のワイヤレス端末の前のハンドオフの結果である。具体的に説明すると、地図情報内のリスティングの一部として第1基地局は、(a)第2基地局の基地局識別子と、(b)第2基地局のネットワークアドレス、例えばそのIPアドレスと、(c)セキュリティ情報、例えば本発明により第1基地局と第2基地局との間の通信を確保するのに用いられる第2基地局のバブリックキーを認識している。207のテスト結果がNOの場合は、第1基地局は第2基地局を認識せずに制御はステップ207に進み、そこで第1基地局はワイヤレス端末に対し、第1基地局は第2基地局を認識せずに、そしてワイヤレス端末はそれ自身の上の第2基地局とのワイヤレスリンク接続をアレンジしなければならない。これは例えば、ワイヤレス端末がその基地局のよりサービスされているセル内で最初に電源が入れた時に、基地局との初期のワイヤレスリンクを確立するのに、ワイヤレス端末が用いる同一のプロセスを用いることにより行われる。

【0024】ステップ203のテスト結果がNOの場合は、ワイヤレス端末から第1基地局への接続が打ち切られるか、あるいはステップ209の後制御はステップ211に進み、そこでワイヤレス端末は、第2基地局がワイヤレス端末とワイヤレスリンクを確立するようリクエストする。このリクエストに応答して条件ブランチポイ

10

20

30

40

50

ント212では、第2基地局は、第2基地局が第1基地局を認識しているか否かを決定する。ステップ212のテスト結果がNOの場合には第2基地局は、第1基地局を認識していないことを示し、制御は213に進み、そこで第2基地局は、ワイヤレス端末を認証しようと試みて、この試みでは図1のセキュリティセンタ119内に記憶された情報の参照を必要とする。その後制御はステップ215に進み、プロセスは以下に説明するよう継続される。ステップ212におけるテスト結果がYESの場合、制御は214に進み、そこでワイヤレスに対するセキュリティ情報が第1基地局で要求され、そこから本発明にしたがって第2基地局が受信する。好ましいことに、第1基地局をすでに認識している第2基地局は、セキュリティセンタによるワイヤレス端末の認証に関わる必要はない。このため、ハンドオフプロセスの容易さかなりの時間が節約できる。通常行われることであるため図2には示してはいないが、第1基地局でセキュリティ情報が得られない場合には、第1基地局が利用できるセキュリティ情報の全てが使用し尽くされ、制御はステップ213に進む。

【0025】ステップ207のテスト結果がYESの場合、基地局は第2基地局を認識していることを示し、制御は条件ブランチポイント208に進み、そこでは第1基地局は、第2基地局により用いられるワイヤレス端末に関連するセキュリティ情報が得られるか否かを決定するためにテストする。このようなセキュリティ情報は、チャレンジャーレスポンス認証対および／またはワイヤレス端末に関連する暗号化キー等である。ステップ208のテスト結果がNOの場合、第1基地局は、第2基地局により使用することのできるワイヤレス端末に関連するセキュリティ情報が得られないことを示し、制御はステップ209に進み、プロセスは上記したように継続する。ステップ208のテスト結果がYESの場合には、第1基地局は第2基地局により使用することのできるワイヤレス端末に関連するセキュリティ情報が得られたことを示し、制御はステップ221に進み、そこで第1基地局は本発明により、例えば自分自身に調和して利用可能なセキュリティ情報を第2基地局に送る。セキュリティ情報の送信は、第1基地局から第2基地局へのワイヤレス端末のハンドオフのリクエストとして第2基地局で

【0026】次にステップ223において、ワイヤレス端末は、第2基地局がワイヤレス端末とのワイヤレスリンクを確立するよう要求する。その後、あるいはステップ214の実行後、制御は条件ブランチポイント225に進み、そこでワイヤレス端末は、第1基地局とデータ

を通信するために、暗号技術を用いているか否かを決定するためにテストする。ステップ225のテスト結果がNOの場合、基地局とデータを通信するためにワイヤレス端末は、暗号リンクを使用していないことを表し、制御はステップ227に進み、そこで第2基地局はワイヤレス端末を認証するために第1基地局から得たセキュリティ情報を用いる。その後条件ブランチポイント215は、ワイヤレス端末が成功裏に認証されたか否かを決定するためにテストする。

【0027】ステップ215のテスト結果がYESの場合、ワイヤレス端末は、通信するために基地局を用いることが許されたことを示し、制御はステップ231に進み、そこでワイヤレス端末は、ユーザトラフィックを第2基地局の搬送するために接続される。その後プロセスは、ステップ233で終了する。ステップ215のテスト結果がNOの場合、ワイヤレス端末は通信用に基地局を利用することが許されないことを示し、制御はステップ233に進み、プロセスはそこで終了する。

【0028】ステップ225のテスト結果がYESの場合、暗号化リンクが基地局とデータを通信するためにワイヤレス端末により使用されていることを示し、制御はステップ229に進み、そこでデータプロセスの暗号化と脱暗号化がワイヤレス端末と第2基地局との間で開始される。このための暗号化アルゴリズムが初期化される。ユーザデータがいったん流れ出すと、暗号化あるいは脱暗号化が適宜自動的に行われる。第1基地局から第2基地局へ渡された新たな暗号化キーの暗号化リンクの使用は、ワイヤレス端末を受領するために行われたハンドオフでは関係しなかった基地局のセル内での活性化に基づいて、ワイヤレス端末が認証された後、ワイヤレス端末の直接的な再認証として同じ目的を達成する。

【0029】次に制御はステップ231に進み、そこでワイヤレス端末は、ユーザトラフィックを搬送するために第2基地局に接続される。このステップの一部として、ワイヤレス端末に第1基地局を介してデータが送信されるネットワークの他の部分は、ワイヤレス端末の第2基地局を介して、例えば公知のモバイルインターネットプロトコルの技術を用いて、新たにデータを転送するために指示される。その後プロセスはステップ233で

【0030】ステップ207のテスト結果がYESの場合、第2基地局は同様に第1基地局を知っており、これは非日常的なエラーの場合では真実ではない。このようなエラーは、実行されるハンドオフに参加するために、第2基地局の拒否により開始され、スムーズには実行されないハンドオフを行うために、ステップ209に制御が進むプロセスを必要とする。

【0031】第1基地局は第2基地局に、第1基地局が最初に受領したセキュリティ情報の全てを送る必要はない。この理由は、第1基地局は、ワイヤレス端末と通信

10

20

30

40

50

11

する際にそのセキュリティ情報の一部を用いており、ある種のセキュリティ情報、例えばチャレンジ-応答対、あるいは符号化キーを使用する良好な試作であるセキュリティ攻撃を未然に防ぐのを助ける。さらにまた、第1基地局により得られたセキュリティ情報は、セキュリティセンタあるいは他の別の基地局から得ることもできる。

【図面の簡単な説明】

【図1】本発明によるネットワーク構成を表す図。

【図2】本発明により図1の基地局間でハンドオフを実行するフローチャート図。

【符号の説明】

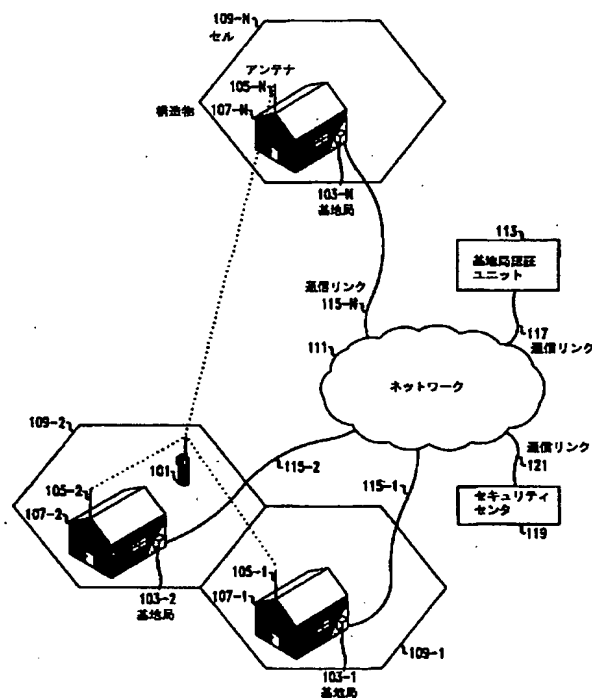
101 ワイヤレス端末
103 基地局
105 アンテナ
107 構造物
109 セル
111 ネットワーク
113 基地局認証ユニット
115、117、121 通信リンク
119 セキュリティセンタ
201 開始 203 第1基地局への接続が存在するか
205 ワイヤレス端末は第1基地局から第2基地局へのハンドオフをリクエストする

*

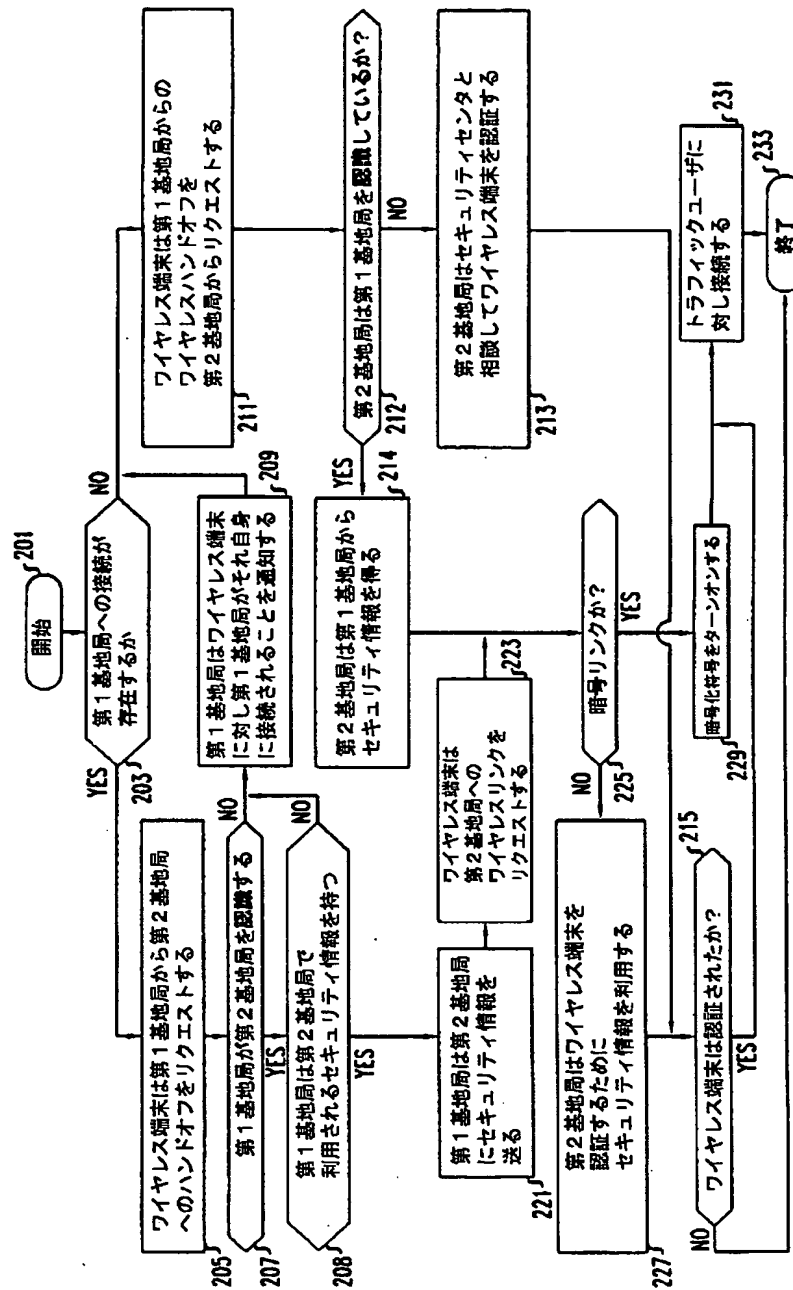
12

* 207 第1基地局が第2基地局を認識する
208 第1基地局は第2基地局で利用されるセキュリティ情報を持つ
209 第1基地局はワイヤレス端末に対し第1基地局がそれ自身に接続されることを通知する
211 ワイヤレス端末は第1基地局からのワイヤレスハンドオフを第2基地局からリクエストする
212 第2基地局は第1基地局を認識しているか？
213 第2基地局はセキュリティセンタと相談してワイヤレス端末を認証する
214 第2基地局は第1基地局からセキュリティ情報を得る
215 ワイヤレス端末は認証されたか？
221 第1基地局は第2基地局にセキュリティ情報を送る
223 ワイヤレス端末は第2基地局へのワイヤレスリンクをリクエストする
225 暗号リンクか？
227 第2基地局はワイヤレス端末を認証するためにセキュリティ情報を利用する
229 暗号化符号をターンオンする
231 トラフィックユーザに対し接続する
233 終了

【図1】



【図2】



フロントページの続き

(71)出願人 596077259

600 Mountain Avenue,
Murray Hill, New Je
rsey 07974-0636U. S. A.

(72)発明者 ステファン ウィリアム デイビース
カナダ国、M5S 2H9 トロント、ス
バンディナ アベニュー アpartment
2 661

(72)発明者 ミカエラ シー、バンダービー
アメリカ合衆国、07738 ニュージャージ
ー、リンクロフト、ウィロー グローブ
ドライブ 114